<u>IN THE CLAIMS</u>

Please amend the claims as follows:

1.   (original)   A method of authenticating a password that is presentable in a series of instances and has a first set of fields (201, 203) and has a second field (113, 114, 202, 311, 313, 314), wherein the first set of fields comprises at least one of (a) a static field (105, 201 or 302)   that does not change upon each instance of the password and (b) a dynamic field (101, 102, 203, 305 or 306) that changes with each instance of the password based upon extrinsic data, and wherein the second field is arranged to contain historic data that is a function of a preceding instance of authentication, the method comprising:

    receiving a current presented instance of the password (110 or 310); and

    performing a comparison operation (605) in which the second field (113, 114, 311, 313 or 314) of the current presented instance of the password is compared using data retained since a prior instance of authentication of the password.

2.   (original)   A method according to claim 1, wherein the historic data is a function of a preceding password.

3. (currently amended) A method according to claim 1 ~~or 2~~,
wherein the historic data is a function of an event record of a
preceding instance of authentication.

4. (currently amended) A method according to claim 1~~, 2 or 3~~,
wherein the first set of fields comprises a static field (201) and
a dynamic field (203).

5. (original) A method according to claim 4, wherein, for the
dynamic field, the step of performing a comparison operation
comprises receiving extrinsic data in the form of date and/or time
and/or place data and/or internet protocol address of a client
machine.

6. (currently amended) A method according to ~~any one of the preceding claims~~claim 1, further comprising, upon successful
comparison, retaining data for purposes of comparison of a next
instance of the password.

7. (original) A method according to claim 6, wherein the data
retained (602) comprises one of the date and the time of receipt of
the instance of the current presented instance of the password.

8.   (original)   A method according to claim 6, wherein the data retained (602) is derived from the place of receipt of the instance of the current presented instance of the password.

9.   (original)   A method according to claim 6, wherein the data retained comprises at least a part of the current presented instance of the password.

10.   (currently amended)   A method according to ~~any one of the preceding claims~~claim 1, wherein the step of comparing comprises:

      generating (604) at least the second field of a generated instance of the password; and

      comparing (605) the second field of the current presented instance of the password with the second field of the generated instance of the password.

11.   (original)   A method according to claim 1, in which the password further has a third field containing pseudo-random data.

12.   (original)   A method according to claim 11, in which the pseudo-random data is input by the user.

13. (currently amended) A method according to claim 11 ~~or 12~~, in which the data retained is the contents of the third field.

14. (currently amended) A method according to claim 6 ~~and 13~~, comprising retaining the contents of the third field.

15. (original) Apparatus for receiving and authenticating a password that is presentable in a series of instances and has a first set of fields (201, 203) and has a second field (202), wherein the first set of fields comprises at least one of (a) a static field (201) that does not change upon each instance of the password and (b) a dynamic field (203) that changes with each instance of the password based upon extrinsic data, and wherein the second field (202) is arranged to contain historic data that is a function of a preceding instance of authentication, the apparatus comprising:

input means (500) for inputting a current presented instance of the password; and

comparison means (501) for performing a comparison operation in which the second field of the current presented instance of the password is compared using data retained since a prior instance of authentication of the password.

16. (original) Apparatus according to claim 15, wherein the historic data is a function of a preceding password.

17. (original) A data carrier having stored thereon instructions and data which, when loaded into the memory (521) of a suitable computer (501), and when presented with a current presented instance of a password that is presentable in a series of instances and has a first set of fields (201, 203) and has a second field (202), wherein the first set of fields comprises at least one of (a) a static field (201) that does not change upon each instance of the password and (b) a dynamic field (203) that changes with each instance of the password based upon extrinsic data, and wherein the second field (202) is arranged to contain data that is a function of a preceding instance of authentication, cause the computer to:

perform a comparison operation (605) in which the second field of the current presented instance of the password is compared using data retained since a prior instance of authentication of the password.